REMARKS

The Office Action dated September 30, 2005 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto. Applicants wish to thank the Examiner for extending the courtesy of an Interview with Applicants' Representative on December 15, 2005. Although no specific agreement was reached, the discussions were helpful and are summarized in this Response. Claims 1-21 are pending in the present application and respectfully are submitted for consideration.

Claims 1-21 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Li et al.* (U.S. Patent No. 6,219,793) in view of *Hoffstein et al.* (U.S. Patent No. 6,076,163). The Office Action took the position that *Li et al.* taught all the features of the claims except "generating a set of subscriber specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in a known mobile communication system." The Office Action then alleged that *Hoffstein et al* taught those features missing from *Li et al.* Applicants respectfully traverse the obviousness rejection and submit that *Li et al.* and *Hoffstein et al.*, either alone or in combination, do not disclose or suggest all the features of any of the presently pending claims.

Claim 1, upon which claims 2-9 are dependent, recites an authentication method for a telecommunications network. The method includes generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner

as in a known mobile communications system. The method also includes transmitting at least some of the challenges contained in the authentication data blocks to the terminal. The method also includes choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communications system. The method also includes determining an authenticator with an aid of the chosen key in the terminal. The method also includes transmitting, from the terminal to the network, the authenticator in a data unit. The data unit contains information relating to the manner in which the authentication is formed and notifying the network of which key corresponding to which challenge was chosen. The method also includes determining a check value with the aid of the chosen key in the network. The method also includes comparing the check value with the authenticator.

Claim 10, upon which claims 11-13 are dependent, recites an authentication system for a telecommunications network. The authentication system includes a terminal of the network and first message transmission means for transmitting an authenticator and a data unit to the network. The data unit includes information relating to the manner in which the authenticator is formed. The authentication system also includes checking means for determining a check value with aid of the data unit. The terminal of the network includes such an identification unit, which receives as input a challenge from which a response and a key are defined essentially in the same manner as in a subscriber

identity module of a main mobile communications system. The system also includes generating means for generating authentication data blocks in the same manner as in the mobile communications systems. The authentication data blocks include a challenge, a response and a key. The system also includes transmission means for transmitting challenges contained by the authentication data blocks to the terminal. The terminal includes selection means for selecting one challenge per use. The first message transmission means inserts such a value into the data unit which indicates which key corresponding to which challenge was selected for use in the terminal. The first message transmission means determine the authenticator and the checking means determine the check value based on the selected key.

Claim 14, upon which claims 15-16 are dependent, recites an authentication method for a telecommunications network. The method. includes generating a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key. The method also includes transmitting at least some of the challenges contained in the authentication data blocks to a terminal. The method also includes receiving an authenticator and a data unit containing information relating to a manner in which the authenticator is formed from the terminal. The method also includes determining based on said data unit which challenge was chosen by the terminal. The method also includes determining a check value with a key corresponding to the chosen challenge. The check value is compared with the authenticator.

Claim 17, upon which claims 18 and 19 are dependent, recites an authentication method for a terminal. The method includes receiving a set of challenges from a telecommunications network. The method also includes choosing one challenge from the set of challenges. The method also includes determining a response and a key based on the chosen challenge. The method also includes determining an authenticator based on the key corresponding to the chosen challenge. The method also includes transmitting the authenticator and the data unit to the telecommunications network. The data unit relates to the manner in which the authenticator is formed. The method also includes notifying the telecommunications network of the chosen challenge.

Claim 20 recites a telecommunications network configured to generate a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key. The network also is configured to transmit at least some of the challenges contained in the authentication data blocks to a terminal. The telecommunications network also is configured to receive an authenticator and a data unit containing information relating to a manner in which the authenticator is formed. The telecommunications network also is configured to determine based on the data unit which challenge was chosen by the terminal. The telecommunications network also is configured to determine a check value with the key correspondent to the chosen challenge. The check value is compared with the authenticator.

Claim 21 recites terminal for a telecommunications network. The terminal is configured to receive a set of challenges from a telecommunications network. The

terminal is also configured to choose one challenge from a set of challenges. The terminal also is configured to determine a response and a key based on the chosen challenge. The terminal also is configured to determine an authenticator based on the key corresponding to the chosen challenge. The terminal also is configured to transmit the authenticator and the data unit to the telecommunications network. The data unit relating to the manner in which the authenticator is formed and notifies the telecommunications network of the chosen challenge.

As discussed in the specification, examples of the present invention enable the use of a known authentication method of a telecommunications network for producing an authenticator for a terminal. Examples of the present invention enable a terminal to receive a challenge and to determine a corresponding key and response. The response is sent from the terminal to the network, where the response received from the terminal is compared to the response calculated in the network. If these two responses are equal, the terminal is successfully authenticated. Thus, it is possible to share a secret key between the terminal and the network for calculating an authenticator in the terminal and for checking the authenticator network. The authenticator may be calculated using any method, which has been, for example, agreed upon before hand. The network is notified about the chosen challenge using a data unit. Applicants respectfully submit that Li and Scott, either alone or in combination, fail to disclose or suggest all the features of any of the presently pending claims. Therefore, *Li et al.* and *Hoffstein et al.* fail to provide the critical and unobvious advantages discussed above.

Li et al. relates to a method of using fingerprints to authenticate wireless communications. Figure 5 of *Li et al.* shows software processing steps for fingerprint matching. A contrasting algorithm reduces all the gray shades of a captured image 502 to either black for ridgelines or white for valley lines, as shown in image 504. A thinned image 506 is examined by further algorithms in step 507 that attempt to deduce and accurately extract the minutiae and their locations as shown in a map 508. Figure 6 of *Li et al.* shows a diagram of central authentication system (CAS) 106. CAS 106 includes a memory 605 including a persistently stored program 606 and various temporarily stored items including a challenge 607, a response token 608, and a decrypted message 609. Program 606 contains instructions for generating a challenge, encrypting the challenge with a fingerprint based token, validating a decrypted challenge by comparison with the generated challenge, fingerprint matching based on tokens, and comparing a response token with one or more stored tokens to assure that tokens are not identical to imply illegal use.

Hoffstein et al. is directed to methods and an apparatus for providing secure user identification or digital signatures based on evaluation of constrained polynomials. A prover sends a verifier a commitment signal representative of a first polynomial satisfying a first set of constraints. The verifier sends the prover a challenge signal representative of a second polynomial satisfying a second set of constraints. The prover generates a response signal as a function of (i) information used to generate the commitment signal, (ii) a challenge signal, and (iii) a private key polynomial of the

prover, such that the response signal is representative of a third polynomial satisfying a third set of constraints. It is noted that "a response" is sent that is a function of several components, but those components themselves are NOT sent. The verifier receives the response signal from the prover, and authenticates the identity of the prover.

Claim 1 recites, in part, "generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key," where method also includes transmitting at least some of the challenges contained in the authentication data blocks to the terminal. Claims 10, 14, 17, 20 and 21, though having different elements and being different in scope, all recite a similar feature. As discussed above, it is clear that *Hoffstein et al.* does not teach or suggest transmitting a key with the challenge. Given this lack of disclosure, *Hoffstein et al.* cannot be used to teach or suggest what has been alleged in the rejection.

As discussed in the Interview, *Hoffstein et al.* fails to disclose the exchange of keys, although the Examiner asserted, during that Interview, that keys must be exchanged to accomplish encryption. To establish a *prima facie* case of obviousness, there must be some motivation or suggestion, either in the references themselves or within the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. The fact that a given modification would have been "well within the ordinary skill in the art" is not sufficient to establish a *prima facie* case of obviousness. Ex parte Levengood, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993). Just because an aspect of the invention may be "obvious to try" does not provide the

proper motivation under §103. M.P.E.P. 2145. In addition, it is also asserted that key exchange could occur separately from the transmission of the challenge, so that there would be no need to send a key along with the challenge.

Applicants also wish to point out that even if key exchange is somehow inherently disclosed in *Hoffstein et al.*, that would still not teach or suggest the transfer of a data block containing a challenge, a response and a key. During the Interview, the Examiner acknowledged that he could not point to any such description in *Hoffstein et al.* Thus, for at least this reason, Applicants respectfully assert that the rejection is improper and should be withdrawn.

Additionally, claim 1 recites, in part, that at least some of the challenges contained in the authentication data blocks to the terminal are transmitted and that the terminal chooses one of the challenges for use in the terminal. Similar subject matter is also found in claims 10, 14, 17, 20 and 21. During the Interview, Applicant's Representative pointed out that *Li et al.* does not teach or suggest the transmission of multiple challenges, from which the terminal chooses one of those challenges. In response, it was alleged that the tokens, derived from fingerprints of users, as discussed in *Li et al.*, were equivalent to the challenges and the wireless telephone chooses one of those tokens.

Applicants respectfully assert that "challenges" are already disclosed in *Li et al.* and are discussed in the same manner as they are discussed in the instant application. Since *Li et al.* already discussed the use of challenges, there would be no reason to view the tokens, which are not disclosed as being challenges or equivalents thereof, as

challenges. Applicants respectfully assert that one of ordinary skill in the art would not have viewed the tokens as challenges since *Li et al.* already disclosed them. As such, Applicants respectfully assert that *Li et al.* cannot teach or suggest what was alleged in the rejection and that the rejection should be withdrawn as being improper.

Applicants also respectfully assert that even if the tokens were accepted as being equivalent to challenges, which Applicants do not accept, those tokens in *Li et al.* are not sent out in multiples from the wireless carrier. Claim 1, and the other independent claims, recite that multiple challenges are sent out and that one is selected by the terminal. Thus, *Li et al.* would still not teach or suggest what has been alleged in the rejection. Therefore, for at least this reason, Applicants respectfully assert that the rejection is improper and should be withdrawn.

In addition, the Office Action also rejects claims 10-21 on the grounds that they relate substantially to the same subject matter as claim 1. Applicants agree that those claims have some similar elements, such that claims 10 and 14 recite "authentication data blocks containing a challenge, a response and a key," transmitting at least some challenges . . . to the terminal," "determining which challenge was chosen by the terminal" and "indicating which key corresponding to which challenge by a determining check value." As discussed above, however, Applicants respectfully assert that these elements are neither taught nor suggested by *Li et al.* and *Hoffstein et al.*

With respect to claims 17 to 21, those claims are specifically directed to the operation of the terminal itself. The terminal in *Li et al.* is capable of generating a local

fingerprint based token, decrypting an encrypted challenge and returning a response which contains the decrypted message (from the challenge) and the locally generated token. The capabilities of the wireless telephone are discussed at column 12, lines 8 to 28 of *Li et al.* It simply does not have the steps recited or the features of the terminal recited in claims 17 and 22 relating to receiving multiple challenges, choosing a challenge from the set of challenges, determining an authenticator based on a chosen key and transmitting the authenticator to the network.

Also, claim 20 is directed to a telecommunications network which is configured to carry out a specific set of steps on the network side. These steps are not disclosed in *Li et al.* The capabilities of the network side in *Li et al.* are discussed in column 15, lines 49 to 60 which discusses program 606 of the CAS 202. This program is not able to carry out the steps recited in claim 20, specifically to generate a set of subscriber specific data blocks, to transmit plural challenges, to receive an authenticator, to determine which challenge was chosen and to determine a check value with a key corresponding to the chosen challenge.

With respect to the additional features of the dependent claims, the cited sections of *Li et al.* and *Hoffstein et al.* fail to teach or suggest the elements of those claims. Because the cited references, either alone or in combination, do not disclose or suggest all the features of independent claims 1, 10, 14, 17, 20 and 21, then claims 1-21 are not rendered obvious. The dependent claims also are not disclosed or suggested by the cited references at least because of their dependency upon the independent claims, and the fact

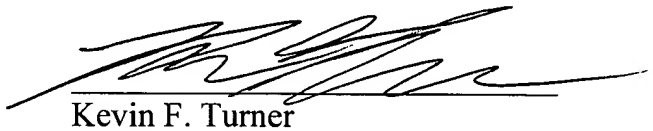
that they recite additional subject matter not disclosed or suggested by the cited references. Applicants respectfully request that the obviousness rejection of claims 1- 21 be withdrawn.

Applicants submit that each of claims 1-21 recite subject matter that is neither disclosed nor suggested by the cited references, either alone or in combination. Applicants respectfully request that all of claims 1-21 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Kevin F. Turner
Registration No. 43,437

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802
KFTjf